Супроводження комплексної системи захисту інформації

Рекомендації щодо структури та змісту Плану захисту інформації в автоматизованій системі

Виконала:
студентка групи СН-41
Чура Наталя

Тернопіль 2011

План захисту інформації в автоматизованих системах (АС) — це набір документів, згідно з якими організують захист інформації протягом життєвого циклу АС.

План захисту містить такі пункти:

- завдання захисту інформації в АС;
- класифікація інформації, що обробляють в АС;
- опис компонентів АС та технології оброблення інформації;
- загрози для інформації в АС;
- політика безпеки інформації в АС;
- система документів із забезпечення захисту інформації в АС.

До завдань захисту інформації в АС належать такі:

- ефективне знешкодження (попереджання) загроз ресурсам АС шляхом комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки;
- забезпечення визначених політикою безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації АС;
- своєчасне виявлення та знешкодження загроз ресурсам АС, причин та умов виникнення порушень функціонування АС та її розвитку;
- створення механізму та умов оперативного реагування на загрози безпеці інформації, інші прояви негативних тенденцій у функціонуванні АС;
- управління засобами захисту інформації, доступом користувачів до ресурсів АС, контроль за їхньою роботою з боку персоналу СЗІ, оперативне сповіщення про спроби НСД до ресурсів АС;
- реєстрація, збирання, зберігання, оброблення даних про всі події в системі, пов'язані з безпекою інформації;
- створення умов для максимально можливого відшкодування та локалізації збитків, що завдають неправомірні (несанкціоновані) дії фізичних та юридичних осіб, вплив зовнішнього середовища та інші чинники, а також зменшення негативного впливу наслідків порушення безпеки на функціонування АС.

Політика безпеки, яку реалізує комплексна система захисту інформації (КСЗІ) для захисту інформації від потенційних внутрішніх та зовнішніх загроз, має охоплювати такі об'єкти захисту:

- відомості (незалежно від виду їхнього подання), що належать до інформації з обмеженим доступом (ІзОД) або інші види інформації, що підлягає захисту, яку обробляють в АС (на паперових, магнітних, оптичних та інших носіях);
- інформаційні масиви і бази даних, програмне забезпечення та інші інформаційні ресурси;
- обладнання АС та інші матеріальні ресурси, зокрема технічні засоби та системи, що не задіяні в обробленні (ІзОД), але розташовані в контрольованій зоні, носії інформації, процеси і технології її оброблення. До технічних областей, в яких необхідно захищати інформаційне та програмне забезпечення, належать робоча станція, комунікаційні канали (фізична мережа) та комутаційне обладнання, сервери, засоби для створення твердих копій даних, накопичувачі інформації;
- засоби і системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту;
- користувачів (персонал) АС, власників інформації та АС, а також їхні права.

Безпеку інформації в АС забезпечують шляхом:

- організації та впровадження системи допуску співробітників (користувачів) до інформації, яка потребує захисту;

- організації обліку, зберігання, обігу інформації, яка потребує захисту, та її носіїв;

- організації та координації робіт із захисту інформації, яка обробляється та передається засобами АС;

- здійснення контролю за забезпеченням захисту інформації, яку обробляють засоби АС, і за збереженням конфіденційних документів (носіїв).

Класифікація інформації:

1. За режимом доступу інформації в АС:

- відкрита - поділяється на таку, що не потребує захисту або захист якої забезпечувати недоцільно, і таку, що потрібно захищати (її цілісність і доступність);

- інформація з обмеженим доступом.

2. За правовим режимом (ІзОД) поділяється:

- таємна

- конфіденційна.

3. За типом її подання в АС.

Інвентаризації підлягають такі об'єкти:

- обладнання — комп'ютерні системи та їх компоненти (процесори, монітори, термінали, робочі станції тощо), периферійні пристрої;

- програмне забезпечення (вихідні, завантажувальні модулі, утиліти, СКБД, операційні системи, діагностичні, тестові програми тощо);

- дані тимчасового і постійного зберігання (інформація на магнітних носіях, друковані, архівні та резервні копії, системні журнали, технічна, експлуатаційна і розпорядча документація тощо);

- персонал і користувачі АС.

На основі Плану захисту інформації в АС складають календарний план робіт із реалізації заходів захисту інформації в АС, який містить такі пункти:

- організаційні заходи;

- контрольно-правові заходи;

- профілактичні заходи;

- інженерно-технічні заходи;

- робота з кадрами.

Список використаних джерел:

1. *Грайворонський М.В., Новіков О.М.* Безпека інформаційно-комунікаційних систем. — К.: Видавнича група BHV, 2009. — 608 с.: іл.

2. *НД ТЗІ 1.4-001-2000:* Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000, № 53 [21].

Дякую за увагу!!!